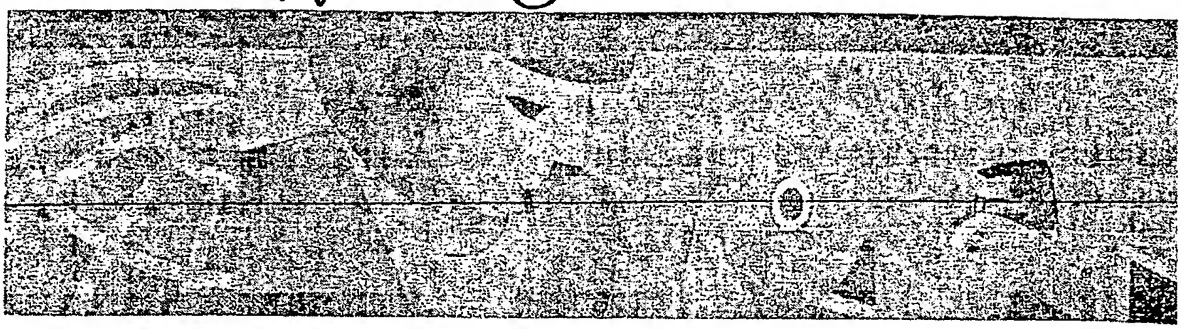


Interdomain Multicast Solutions Using SSM

Version Number	Date	Notes
1	3/22/2001	This document was created.

The current IP multicast infrastructure in the Internet and many enterprise intranets is based on the Protocol Independent Multicast sparse mode (PIM-SM) protocol and Multicast Source Discovery Protocol (MSDP). These protocols have proven to be reliable, extensive, and efficient. However, they are bound to the complexity and functionality limitations of the Internet Standard Multicast (ISM) service model. For example, with ISM, the network must maintain knowledge about which hosts in the network are actively sending multicast traffic. With Source Specific Multicast (SSM), this information is provided by receivers through the source addresses relayed to the last hop routers by Internet Group Management Protocol Version 3 (IGMPv3), IGMP Version 3 lite (IGMP v3lite), or URL Rendezvous Directory (URD). SSM is an incremental response to the issues associated with ISM and is intended to coexist in the network with the protocols developed for ISM. In general, SSM provides a more advantageous IP multicast service than ISM for applications that utilize SSM.

This solutions document describes how an Internet service provider (ISP) customer within an interdomain multicast network implements SSM in its network using URD. The SSM solution presented in this document is based on an actual customer situation. This solution was tested and verified in a lab environment and has been deployed in the field. Alternative ways to implement SSM, such as IGMPv3 and IGMP v3lite host signalling, are discussed but were not implemented in our lab environment.

The scope of this solutions document is to describe basic design and deployment of SSM using URD. It does not discuss in detail the general operation of the protocols associated with developing interdomain multicast networks such as PIM-SM.

This document contains the following sections:

- Customer Business Objectives
- Proposed Solution: URD Host Signalling
- Implementation of Proposed Solution: URD Host Signalling
- Related Documents

Customer Business Objectives

The customer business objectives for deploying IP multicast in a network are as follows:

- To leverage existing network infrastructure to create additional incremental revenue streams and provide value-added services to customers by enabling interdomain multicast.
- To efficiently deliver scalable real-time content (for example, high-quality video and audio, market data, and distance learning) from content providers to subscribers by enabling IP multicast.

The customer business objectives for deploying IP multicast using SSM services, as opposed to Internet Standard Multicast (ISM) services, in a network are as follows:

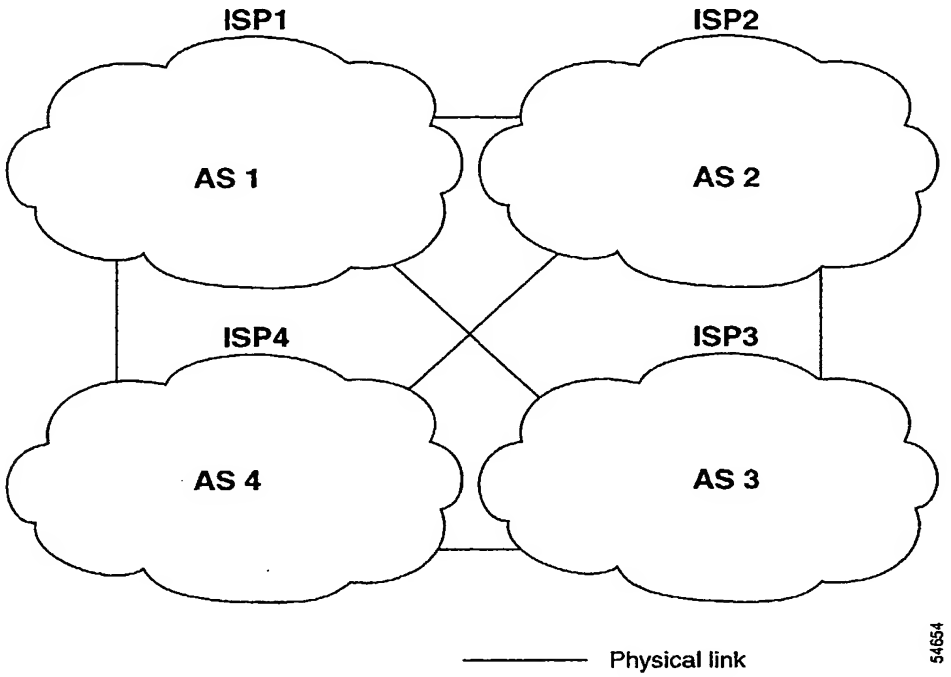
- To reduce the operational complexity of deploying IP multicast and therefore reduce overhead costs.
- To simplify address management and reduce the risk of denial of service attacks.

Initial Interdomain Multicast Network Topology

The SSM network scenario used in this document is based on the hypothetical interdomain ISP network scenario described in the "Interdomain Multicast Solutions Using MSDP" document. Figure 1 shows the logical connections of the initial interdomain multicast network topology. Each ISP in Figure 1 has Border Gateway Protocol (BGP) peering and its own autonomous system (AS) established. The design of each ISP multicast network topology is dependent on the individual requirements of the ISP.

Note The solution presented in this document is based on a hypothetical interdomain ISP environment. All the IP addresses and configuration in this document are provided for illustrative purposes only.

Figure 1 Logical Connections of the Initial Interdomain Multicast Network Topology



Possible Solutions

SSM is a datagram delivery model that best supports one-to-many applications, also known as Interne broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for applications such as audio and video broadcasting. Three possible solutions for implementing SSM with Cisco IOS software are discussed in the following sections:

- Possible Solution 1: IGMPv3 Host Signalling
- Possible Solution 2: IGMP v3lite Host Signalling
- Possible Solution 3: URD Host Signalling

To run SSM with IGMPv3, SSM must be supported in the Cisco IOS router, the host where the application is running, and the application itself. IGMP v3lite and URD are two Cisco-developed transition solutions that enable the immediate development and deployment of SSM services, withou the need to wait for the availability of full IGMPv3 support in host operating systems and SSM receive applications. IGMPv3, IGMP v3lite, and URD interoperate with each other so that both IGMP v3lite and URD can easily be used as transitional solutions toward full IGMPv3 support in hosts.

This section contains the following subsections:

- How SSM Differs from Internet Standard Multicast
- SSM IP Address Range
- SSM Operations

- Possible Solution 1: IGMPv3 Host Signalling
- Possible Solution 2: IGMP v3lite Host Signalling
- Possible Solution 3: URD Host Signalling

How SSM Differs from Internet Standard Multicast

The Internet Standard Multicast (ISM) service is described in RFC 1112, *Host Extensions for IP Multicasting*. This service consists of the delivery of IP datagrams from any source to a group of receivers called the multicast host group. The datagram traffic for the multicast host group consists of datagrams with an arbitrary IP unicast source address S and the multicast group address G as the IP destination address. Systems will receive this traffic by becoming members of the host group. Membership to a host group simply requires signalling the host group through IGMP Version 1, 2, or 3.

In SSM, delivery of datagrams is based on (S, G) channels. Traffic for one (S, G) channel consists of datagrams with an IP unicast source address S and the multicast group address G as the IP destination address. Systems will receive this traffic by becoming members of the (S, G) channel. In both SSM and ISM, no signalling is required to become a source. However, in SSM, receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources. In other words, receivers can receive traffic only from (S, G) channels to which they are subscribed, whereas in ISM, receivers need not know the IP addresses of sources from which they receive their traffic. The proposed standard approach for channel subscription signalling utilizes IGMP INCLUDE mode membership reports, which are supported only in IGMPv3.

SSM IP Address Range

SSM can coexist with ISM service by applying the SSM delivery model to a configured subset of the IP multicast group address range. The Internet Assigned Numbers Authority (IANA) has reserved the address range 232.0.0.0 through 232.255.255.255 for SSM applications and protocols. Cisco IOS software allows SSM configuration for an arbitrary subset of the IP multicast address range from 224.0.0.0 through 239.255.255.255. When an SSM range is defined, existing IP multicast receiver applications will not receive any traffic when they try to use addresses in the SSM range (unless the application is modified to use explicit (S, G) channel subscription or is SSM-enabled through URD).

SSM Operations

An established network in which IP multicast service is based on PIM-SM can support SSM services. SSM can also be deployed alone in a network without the full range of protocols that are required for interdomain PIM-SM (for example, MSDP, Auto-RP, or bootstrap router [BSR]) if only SSM service is needed. However, multiprotocol BGP may be required to maintain IP multicast connectivity if multiple autonomous systems are deployed in a network.

If SSM is deployed in a network already configured for PIM-SM (Cisco IOS Release 12.0 or a later release is recommended), then only the last hop routers must be upgraded to a Cisco IOS Release 12.1(5)T or later release image that supports SSM. Routers that are not directly connected to receivers can run Cisco IOS Release 12.0 or later releases. In general, routers that are not last hop routers must only run PIM-SM in the SSM range, and may need additional access control configuration to suppress MSDP signalling, registering, or PIM-SM shared tree operations from occurring within the SSM range.

In Cisco IOS Release 12.1(3)T and later releases, the SSM mode of operation is enabled by configurir the SSM range through the **ip pim ssm** global configuration command. This configuration has the following effects:

- For groups within the SSM range, (S, G) channel subscriptions are accepted through IGMPv3 INCLUDE mode membership reports, IGMP v3lite, or URD. Each of these methods must be configured on a per-interface basis. IGMP v3lite and URD (S, G) channel subscriptions are ignore for groups outside the SSM range.
- PIM operations within the SSM range of addresses change to PIM source specific mode (PIM-SSM). PIM-SSM is the routing protocol that supports the implementation of SSM and is derived from PIM-SM. In PIM-SSM mode, only PIM (S, G) join and prune messages are generate by the router, and no (S, G) rendezvous point tree (RPT) or (*, G) RPT messages are generated. Incoming messages related to RPT operations are ignored or rejected and incoming PIM registe messages are immediately answered with register-stop messages. PIM-SSM is backward compatible with PIM-SM, unless a router is a last hop router. Therefore, routers that are not last hop routers can run PIM-SM for SSM groups (for example, if they do not yet support SSM).
- No MSDP Source-Active (SA) messages within the SSM range will be accepted, generated, or forwarded.

Possible Solution 1: IGMPv3 Host Signalling

IGMPv3 is the third version of the Internet Engineering Task Force (IETF) standards track protocol used for hosts to signal membership to last hop routers of multicast groups. IGMPv3 introduces the ability for hosts to signal group membership with filtering capabilities with respect to sources, whicl is required for SSM. A host can either signal that it wants to receive traffic from all sources sending t a group except for some specific sources (called EXCLUDE mode), or that it wants to receive traffic only from some specific sources sending to the group (called INCLUDE mode).

IGMPv3 can operate with both ISM and SSM. In ISM, both EXCLUDE and INCLUDE mode report are applicable. In SSM, only INCLUDE mode reports are accepted by the last hop router; EXCLUDI mode reports are ignored.

For more information on IGMPv3, refer to the Cisco IOS Release 12.1(5)T *IGMP Version 3* feature module.

Possible Solution 2: IGMP v3lite Host Signalling

IGMP v3lite is a Cisco-developed transitional solution that allows immediate development of SSM receiver applications switching to IGMPv3 as soon as it becomes available. It enables you to write an run SSM applications on hosts that do not yet support IGMPv3 in their operating system kernel.

Applications must be compiled with the Host Side IGMP Library (HSIL) for IGMP v3lite. This software provides applications with a subset of the IGMPv3 applications programming interface (API that is required to write SSM applications. HSIL was developed for Cisco by Talarian and is availabl on the following website:

http://www.talarianmulticast.com/cgi-bin/igmpdownld

One part of the HSIL is a client library linked to the SSM application. It provides the SSM subset of th IGMPv3 API to the SSM application. If possible, the library checks whether the operating system kernel supports IGMPv3. If it does, then the API calls simply are passed through to the kernel. If the kernel does not support IGMPv3, then the library uses the IGMP v3lite mechanism.

When using the IGMP v3lite mechanism, the library tells the operating system kernel to join to the whole multicast group, because joining to the whole group is the only method for the application to receive traffic for that multicast group (if the operating system kernel only supports IGMPv1 or IGMPv2). In addition, the library signals the (S, G) channel subscriptions to an IGMP v3lite server process, which is also part of the HSIL. A server process is needed because multiple SSM applications may be on the same host. This server process will then send IGMP v3lite-specific (S, G) channel subscriptions to the last hop Cisco IOS router, which needs to be enabled for IGMP v3lite. This Cisco IOS router will then see both the IGMPv1 or IGMPv2 group membership reports from the operating system kernel and the (S, G) channel subscription from the HSIL daemon. If the router sees both of these messages, it will interpret them as an SSM (S, G) channel subscription and join to the channel through PIM-SSM. We recommend referring to the documentation accompanying the HSIL software for further information on how to utilize IGMP v3lite with your application.

Possible Solution 3: URD Host Signalling

URD is a Cisco-developed transitional solution that enables the deployment of SSM with existing IP multicast receiver applications that do not support IGMPv3—the software on the end-user systems running the application need not be updated. URD is a content provider solution in which the receiver applications can be started or controlled through a web browser.

For more information about URD, see the "Proposed Solution: URD Host Signalling" section later in this document.

Proposed Solution: URD Host Signalling

The customer in this proposed solution chose to implement URD because it wanted to immediately deploy SSM services with existing IP multicast receiver applications that do not support IGMPv3. It also did not want to upgrade any software on its end-user systems.

This section contains the following subsections:

- Strategy
- Network Topology
- How This Solution Works
- Benefits
- Ramifications

Strategy

The strategy of this proposed solution assumes that IP multicast using MSDP is already deployed in th autonomous system of the ISP and that IP multicast connectivity exists between ISPs.

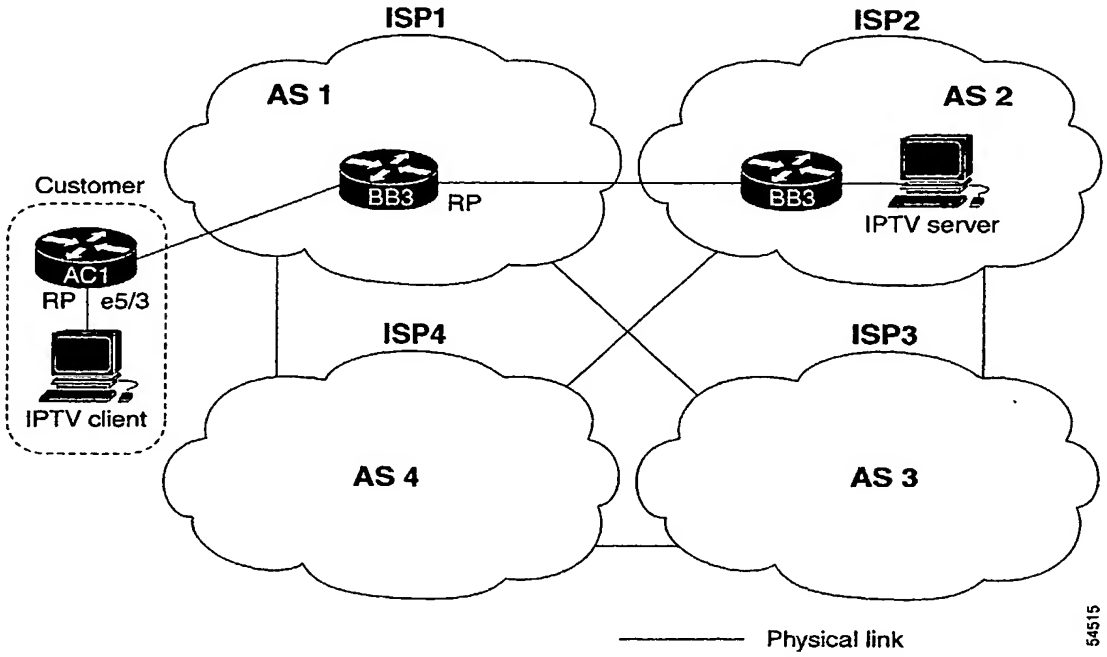
The strategy to deploy SSM with URD is as follows:

- Determine an IP multicast address range to run SSM. The suggested default range is from 232.0.0. through 232.255.255.255.
- Disable rendezvous point (RP) and MSDP peers from processing this SSM address range as ISM services.
- Configure edge devices to process URD host reports.

Network Topology

Figure 2 shows the logical connections of the SSM network topology.

Figure 2 Logical Connections of the Initial SSM Network Topology



How This Solution Works

URD operates by passing a special URL from the web browser to the last hop router. This URL is called a URD intercept URL. A URD intercept URL is encoded with the (S, G) channel subscription and has a format that allows the last hop router to easily intercept it.

As soon as the last hop router intercepts both an (S, G) channel subscription encoded in a URD intercept URL and sees an IGMP group membership report for the same multicast group from the receiver application, the last hop router will use PIM-SSM to join toward the (S, G) channel as long as the application maintains the membership for the multicast group G. The URD intercept URL is thus only needed initially to provide the last hop router with the address of the sources to join to.

A URD intercept URL has the following syntax:

`http://webserver:465/path?group=group&source=source1&...source=sourceN&`

The *webserver* string is the name or IP address to which the URL is targeted. This target need not be the IP address of an existing web server, except for situations where the web server wants to recognize that the last hop router failed to support the URD mechanism. The number 465 indicates the URD port. Port 465 is reserved for Cisco by the IANA for the URD mechanism so that no other applications should use this port.

When the browser of a host encounters a URD intercept URL, it will try to open a TCP connection t the web server on port 465. If the last hop router is enabled for URD on the interface where the route receives the TCP packets from the host, it will intercept all packets for TCP connections destined to port 465 independent of the actual destination address of the TCP connection (independent of the address of the web server). Once intercepted, the last hop router will "speak" a very simple subset o HTTP on this TCP connection, emulating a web server. The only HTTP request that the last hop route will understand and reply to is the following GET request:

```
GET argument HTTP/1.0
argument = /path?group=group&source=source1&...source=sourceN&
```

When it receives a GET request, the router tries to parse the argument according to this syntax to deriv one or more (S, G) channel memberships. The *path* string of the argument is anything up to, but not including, the first question mark, and is ignored. The *group* and *source1* through *sourceN* strings ar the IP addresses or fully qualified domain names of the channels for which this argument is a subscription request. If the argument matches the syntax shown, the router interprets the argument t be subscriptions for the channels (*source1*, *group*) through (*sourceN*, *group*).

The router will accept the channel subscriptions if the following conditions are met:

- The IP address of the multicast group is within the SSM range.
- The IP address of the host that originated the TCP connection is directly connected to the router

If the channel subscription is accepted, the router will respond to the TCP connection with the followin HTML page format:

```
HTTP/1.1 200 OK
Server:cisco IOS
Content-Type:text/html
<html>
<body>
Retrieved URL string successfully
</body>
</html>
```

If an error condition occurs, the <body> part of the returned HTML page will carry an appropriate erro message. The HTML page is a by-product of the URD mechanism. This returned text may, dependin on how the web pages carrying a URD intercept URL are designed, be displayed to the user or be size so that the actual returned HTML page is invisible.

The primary effect of the URD mechanism is that the router will "remember" received channel subscriptions and will match them against IGMP group membership reports received by the host. Th router will remember a URD (S, G) channel subscription for up to 3 minutes without a matching IGM group membership report. When the router sees that it has received both an IGMP group membershi report for a multicast group G and a URD (S, G) channel subscription for the same group G, it will joi the (S, G) channel through PIM-SSM. The router will then continue to join to the (S, G) channel base only on the presence of a continuing IGMP membership from the host. Thus, one initial URD channe subscription is all that needs to be added through a web page to enable SSM with URD.

If the last hop router from the receiver host is not enabled for URD, then it will not intercept the HTT connection toward the web server on port 465. This situation will result in a TCP connection to port 46 on the web server. If no further provisions on the web server are taken, then the user may see a notic (for example, "Connection refused") in the area of the web page reserved for displaying the URD intercept URL (if the web page was designed to show this output). It is also possible to let the web serve "listen" to requests on port 465 and install a Common Gateway Interface (CGI) script that would allo the web server to know if a channel subscription failed (for example, to subsequently return more complex error descriptions to the user).

Because the router returns a Content-Type of text and HTML, the best way to include the URD intercept URL into a web page is to use a frame. By defining the size of the frame, you can also hide the URD intercept URL on the displayed page.

By default, URD is disabled on all interfaces. When URD is configured on an interface using the **ip urd** interface configuration command, it will be active only for IP multicast addresses in the SSM range.

Benefits

The benefits of deploying SSM in a network are as follows:

- IP multicast address management not required

  In the Internet Standard Multicast (ISM) service, applications must acquire a unique IP multicast group address because traffic distribution is based only on the IP multicast group address used. If two applications with different sources and receivers use the same IP multicast group address, then receivers of both applications will receive traffic from the senders of both applications. Even though the receivers, if programmed appropriately, can filter out the unwanted traffic, this situation would cause generally unacceptable levels of unwanted traffic.

  Allocating a unique IP multicast group address for an application is still a problem. Most short-lived applications use mechanisms like Session Description Protocol (SDP) and Session Announcement Protocol (SAP) to get a random address, a solution that does not work well with a rising number of applications in the Internet. The best current solution for long-lived applications is described in RFC 2770, but this solution suffers from the restriction that each autonomous system is limited to only 255 usable IP multicast addresses.

  In SSM, traffic from each source is forwarded between routers in the network independent of traffic from other sources. Thus different sources can reuse multicast group addresses in the SSM range.

- Denial of service attacks from unwanted sources inhibited

  In SSM, multicast traffic from each individual source will be transported across the network only if it was requested (through IGMPv3, IGMP v3lite, or URD memberships) from a receiver. In contrast, ISM forwards traffic from any active source sending to a multicast group to all receivers requesting that multicast group. In Internet broadcast applications, this ISM behavior is highly undesirable because it allows unwanted sources to easily disturb the actual Internet broadcast source by simply sending traffic to the same multicast group. This situation depletes bandwidth at the receiver side with unwanted traffic and thus disrupts the undisturbed reception of the Internet broadcast. In SSM, this type of denial of service attack cannot be made by simply sending traffic to a multicast group.

- Easy to install and manage

  SSM is easy to install and provision in a network because it does not require the network to maintain which active sources are sending to multicast groups. This requirement exists in ISM (with IGMPv1, IGMPv2, or IGMPv3).

  The current standard solutions for ISM service are PIM-SM and MSDP. Rendezvous point (RP) management in PIM-SM (including the necessity for Auto-RP or BSR) and MSDP is required only for the network to learn about active sources. This management is not necessary in SSM, which makes SSM easier to install and manage, and therefore easier to operationally scale in deployment. Another factor that contributes to the ease of installation of SSM is the fact that it can leverage preexisting PIM-SM networks and requires only the upgrade of last hop routers to support IGMPv3, IGMP v3lite, or URD.

- Ideal for Internet broadcast applications

  The three benefits previously described make SSM ideal for Internet broadcast-style applicatio for the following reasons:

  - The ability to provide Internet broadcast services through SSM without the need for unique multicast addresses allows content providers to easily offer their service (IP multicast addre allocation has been a serious problem for content providers).
  - The prevention against denial of service attacks is an important factor for Internet broadcas services because, with their exposure to a large number of receivers, they are the most comm targets for such attacks.
  - The ease of installation and operation of SSM makes it ideal for network operators, especial in those cases where content needs to be forwarded between multiple independent PIM domains (because there is no need to manage MSDP for SSM between PIM domains).

Ramifications

The ramifications for deploying SSM in a network are as follows:

- Legacy applications within the SSM range restrictions

  Existing applications in a network predating SSM will not work within the SSM range, unless the are modified to support (S, G) channel subscriptions or are enabled through URD. Therefore, enabling SSM in a network may cause problems for existing applications if they use addresses within the designated SSM range.

- IGMP v3lite and URD require a Cisco IOS last hop router

  SSM and IGMPv3 are solutions that are being standardized in the IETF. However, IGMP v3lite an URD are Cisco-developed solutions. For IGMP v3lite and URD to operate properly for a host, th last hop router toward that host must be a Cisco IOS router with IGMP v3lite or URD enabled.

  Note This limitation does not apply to an application using the HSIL if the host has kernel support for IGMPv3, because then the HSIL will use the kernel IGMPv3 instead of IGMP v3lite.

- Address management restrictions

  Address management is still necessary to some degree when SSM is used with Layer 2 switchin mechanisms. Cisco Group Management Protocol (CGMP), IGMP Snooping, and Router-Port Group Management Protocol (RGMP) currently support only group-specific filtering, not (S, G) channel-specific filtering. If different receivers in a switched network request different (S, G) channels sharing the same group, then they will not benefit from these existing mechanisms. Instead, both receivers will receive all (S, G) channel traffic (and filter out the unwanted traffic o input). Because of the ability of SSM to reuse the group addresses in the SSM range for many independent applications, this situation can lead to less than expected traffic filtering in a switche network. For this reason it is important to follow the recommendations set forth in the IETF draft for SSM to use random IP addresses out of the SSM range for an application to minimize the chanc for reuse of a single address within the SSM range between different applications. For example, a application service providing a set of television channels should, even with SSM, use a different group for each television (S, G) channel. This setup will guarantee that multiple receivers on different channels within the same application service will never experience traffic aliasing in networks that include Layer 2 switches.

- State maintenance limitations

  In PIM-SSM, the last hop router will continue to periodically send (S, G) join messages if appropriate (S, G) subscriptions are on the interfaces. Therefore, as long as receivers send (S, G) subscriptions, the shortest path tree (SPT) state from the receivers to the source will be maintained, even if the source is not sending traffic for longer periods of time (or even never).

  This case is opposite to PIM-SM, where (S, G) state is maintained only if the source is sending traffic and receivers are joining the group. If a source stops sending traffic for more than 3 minutes in PIM-SM, the (S, G) state will be deleted and only reestablished after packets from the source arrive again through the RPT. Because no mechanism in PIM-SSM notifies a receiver that a source is active, the network must maintain the (S, G) state in PIM-SSM as long as receivers are requesting receipt of that channel.

Implementation of Proposed Solution: URD Host Signalling

This section contains the following subsections:

- Prerequisites and Design Considerations
- Implementation Process Steps
- Device Characteristics and Configuration Files

Prerequisites and Design Considerations

The prerequisite for deploying SSM using URD is to configure interdomain multicast using the following configuration tasks:

- Configure MBGP to exchange multicast routing information.
- Configure multicast borders appropriately.

For more information on how to perform these configuration tasks, refer to the "Interdomain Multica: Solutions Using MSDP" document.

Implementation Process Steps

Note The multicast solutions in this document were tested with valid IP addresses. In the example configurations provided in the following sections, the first octet of these reserved IP addresses has been replaced with the letter "J" or the letter "K" for privacy reasons. The letter "J" always represents one unique number, and the letter "K" always represents one unique number that is different from "J."

The example configurations are intended for illustrative purposes only. The letters "J" and "K" must be replaced with valid numbers when these IP addresses are configured in an actual network.

Note The example configurations provided in the following sections use boldface text to indicate pertinent configuration commands used for deploying the IP multicast solutions described in this document.

The following steps were used to configure SSM using URD on the devices shown in Figure 2:

Step 1 **Select and enable the SSM range in the ISP.**

The following sample configuration shows how to select and enable the SSM range in ISP1:

```
ip pim ssm
```

Step 2 **Configure filters on the RP for PIM-SM and MSDP traffic in the SSM address range.**

The following sample configuration shows how to configure filters on the RP (ISP1BB3 router) for PIM-SM and MSDP traffic in the SSM address range:

```
ip msdp sa-filter in J.4.0.203 list 124
ip msdp sa-filter out J.4.0.203 list 124
```

The following access list is configured on the ISP1BB3 router:

```
access-list 124 deny   ip any host 224.0.2.2
access-list 124 deny   ip any host 224.0.1.3
access-list 124 deny   ip any host 224.0.1.24
access-list 124 deny   ip any host 224.0.1.22
access-list 124 deny   ip any host 224.0.1.2
access-list 124 deny   ip any host 224.0.1.35
access-list 124 deny   ip any host 224.0.1.60
access-list 124 deny   ip any host 224.0.1.39
access-list 124 deny   ip any host 224.0.1.40
access-list 124 deny   ip any 239.0.0.0 0.255.255.255
access-list 124 deny   ip 10.0.0.0 0.255.255.255 any
access-list 124 deny   ip 127.0.0.0 0.255.255.255 any
access-list 124 deny   ip 172.16.0.0 0.15.255.255 any
access-list 124 deny   ip 192.168.0.0 0.0.255.255 any
access-list 124 deny   ip any 232.0.0.0 0.255.255.255
```

Step 3 **Configure URD on user interfaces.**

The following sample configuration shows how to configure URD on Ethernet5/3 on the ISP1AC1 router. The **ip urd** interface configuration command enables interception of TCP packets sent to the reserved URD port 465 on an interface and processing of URD channel subscription reports.

```
ISP1AC1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ISP1AC1(config)# interface Ethernet 5/3
ISP1AC1(config-if)# ip urd
ISP1AC1(config-if)#
```

Step 4 **Verify that URD clients can connect to a source. (Optional)**

a. **Enable debug output and attempt to connect to a source:**

```
ISP1AC1# debug ip igmp 232.0.2.1
ISP1AC1# debug ip igmp 232.0.2.2
ISP1AC1# debug ip urd
ISP1AC1# debug ip mrouting

Mar 7 14:17:37 PST:URD:Intercepted TCP SYN packet from K.250.1.41,
0:772431754(ack:seq)
Mar 7 14:17:37 PST:URD:Intercepted TCP ACK packet from K.250.1.41,
48154099:772431755(ack:seq)
Mar 7 14:17:37 PST:URD:Data intercepted from K.250.1.41, offset 5
Mar 7 14:17:37 PST:URD:Enqueued
string:'/cgi-bin/error.html?group=232.0.2.2&port=22306&source=J.2.11.6&lifet'
Mar 7 14:17:37 PST:URD:Dequeued URD packet, len:137
Mar 7 14:17:37
PST:URD:String:/cgi-bin/error.html?group=232.0.2.2&port=22306&source=J.2.11.6&lifetim
e=7200&group=232.0.2.1&port=49254&source=J.2.11.6&lifetime=7200
Mar 7 14:17:37 PST:URD:Matched token:group
Mar 7 14:17:37 PST:URD:Parsed value:232.0.2.2
Mar 7 14:17:37 PST:URD:Matched token:source
Mar 7 14:17:37 PST:URD:Parsed value:J.2.11.6
Mar 7 14:17:37 PST:URD:Matched token:lifetime
Mar 7 14:17:37 PST:URD:Parsed value:7200
Mar 7 14:17:37 PST:URD:Matched token:group
```

```
Mar 7 14:17:37 PST:URD:Parsed value:232.0.2.1
Mar 7 14:17:37 PST:URD:Matched token:source
Mar 7 14:17:37 PST:URD:Parsed value:J.2.11.6
Mar 7 14:17:37 PST:URD:Matched token:lifetime
Mar 7 14:17:37 PST:URD:Parsed value:7200

Mar 7 14:17:37 PST:URD:Creating IGMP source state for group 232.0.2.2
Mar 7 14:17:37 PST:IGMP:Setting source flags 18 on (J.2.11.6,232.0.2.2)

Mar 7 14:17:37 PST:URD:Creating IGMP source state for group 232.0.2.1
Mar 7 14:17:38 PST:MRT:Create (J.2.11.6/32, 232.0.2.1), RPF
FastEthernet3/0/K.250.1.1, PC 0x609E5CA0
Mar 7 14:17:38 PST:MRT:Add/Update Ethernet5/3/232.0.2.1 to the olist of (J.2.11.6,
232.0.2.1), Forward state
Mar 7 14:17:38 PST:MRT:Create (K.250.1.41/32, 232.0.2.1), RPF Ethernet5/3/0.0.0.0, P(
0x609F25FC

Mar 7 14:17:39 PST:IGMP:Received v2 Report on Ethernet5/3 from K.250.1.41 for
232.0.2.2
Mar 7 14:17:39 PST:MRT:Create (J.2.11.6/32, 232.0.2.2), RPF
FastEthernet3/0/K.250.1.1, PC 0x609E5CA0
Mar 7 14:17:39 PST:MRT:Add/Update Ethernet5/3/232.0.2.2 to the olist of (J.2.11.6,
232.0.2.2), Forward state
Mar 7 14:17:39 PST:MRT:Create (K.250.1.41/32, 232.0.2.2), RPF Ethernet5/3/0.0.0.0, P(
0x609F25FC
```

b. Verify that SSM flags are set:

```
ISP1AC1# show ip mroute

IP Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Advertised via MSDP, U - URD,
       I - Received Source Specific Host Report
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 224.0.1.40), 00:01:55/00:00:00, RP K.250.0.201, flags:SJCL
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Loopback0, Forward/Sparse, 00:01:55/00:02:59

(J.2.11.6, 232.0.2.2), 00:00:45/00:02:59, flags:sCTUI
  Incoming interface:FastEthernet3/0, RPF nbr K.250.1.1
  Outgoing interface list:
    Ethernet5/3, Forward/Sparse, 00:00:16/00:02:46

(K.250.1.41, 232.0.2.2), 00:00:45/00:02:14, flags:sPCT
  Incoming interface:Ethernet5/3, RPF nbr 0.0.0.0
  Outgoing interface list:Null
```

Configuration Files

```
!
version 12.1
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
!
hostname ISP1AC1
!
logging buffered 1000000 debugging
logging rate-limit console 10 except errors
aaa new-model
aaa authentication login default group tacacs+ enable
aaa authentication login NOTACACS enable
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
enable password lab
!
clock timezone PST -8
clock summer-time PST recurring
ip subnet-zero
ip cef
!
!
ip multicast-routing
call rsvp-sync
!
!
interface Loopback0
 ip address K.250.0.201 255.255.255.255
 ip pim sparse-mode
!
interface FastEthernet3/0
 description To ISP1DA1, FA0/1/0
 ip address K.250.1.2 255.255.255.248
 ip pim bsr-border
 ip pim sparse-mode
 ip multicast boundary 1
 duplex full
!
interface Ethernet5/2
 description TO ISP1AC1IPTV
 ip address K.250.1.33 255.255.255.248
 ip pim sparse-mode
 duplex half
!
interface Ethernet5/3
 description TO ISP1AC1CL1
 ip address K.250.1.41 255.255.255.248
 ip pim sparse-mode
→ ip urd
 duplex half
!
ip classless
ip route 0.0.0.0 0.0.0.0 K.250.1.1
no ip http server
ip pim rp-address K.250.0.201
ip pim ssm default
ip msdp peer J.1.0.203 connect-source FastEthernet3/0
ip msdp sa-filter in J.1.0.203 list 124
ip msdp sa-filter out J.1.0.203 list 124
ip msdp cache-sa-state
ip msdp redistribute list 124
```

Device Characteristics and Configuration Files

This section includes the device characteristics and configuration files for the following host names:

- ISP1AC1
- ISP2BB3
- ISP1BB3

Note The multicast solutions in this document were tested with valid IP addresses. In the example configurations provided in the following sections, the first octet of these reserved IP addresses has been replaced with the letter "J" or the letter "K" for privacy reasons. The letter "J" always represents one unique number, and the letter "K" always represents one unique number that is different from "J."

The example configurations are intended for illustrative purposes only. The letters "J" and "K" must be replaced with valid numbers when these IP addresses are configured in an actual network.

Note The example configurations provided in the following sections use boldface text to indicate pertinent configuration commands used for deploying the IP multicast solutions described in this document.

ISP1AC1

Device Characteristics

Table 1 shows the device characteristics for ISP1AC1.

Table 1 Hardware and Software Device Characteristics for ISP1AC1

Host name	ISP1AC1
Chassis type	Cisco 7206VXR router
Physical interfaces	• 8 Ethernet/IEEE 802.3 • 3 Fast Ethernet/IEEE 802.3
Hardware components	Cisco 7206VXR (NPE300) processor
Software loaded	Cisco IOS Release 12.1(5)T
Memory	Cisco 7206VXR (NPE300) processor (revision D): 40 MB
IP addresses	• Loopback0: K.250.0.201 255.255.255.255 • FastEthernet3/0: K.250.1.2 255.255.255.248 • Ethernet5/2: K.250.1.33 255.255.255.248 • Ethernet5/3: K.250.1.41 255.255.255.248

ISP2BB3

Device Characteristics

Table 2 shows the device characteristics for ISP2BB3.

Table 2 Hardware and Software Device Characteristics for ISP2BB3

Host name	ISP2BB3
Chassis type	Cisco 12008 Gigabit Switch Router (GSR)
Physical interfaces	• 1 Ethernet/IEEE 802.3 • 1 Gigabit Ethernet/IEEE 802.3 • 7 Packet Over SONET (POS)
Hardware components	• Cisco 12008/GRP (R5000) processor (revision 0x01) • 1 Route Processor card • 1 clock scheduler card • 3 switch fabric cards • 1 four-port OC-3 POS controller (4 POS) • 3 OC-48 POS E.D. controllers (3 POS) • 1 single-port Gigabit Ethernet/IEEE 802.3z controller (1 Gigabit Ethernet)
Software loaded	Cisco IOS Release 12.0(13)S2
Memory	Cisco 12008/GRP (R5000) processor (revision 0x01): 128 MB
IP addresses	• Loopback0: J.2.0.203 255.255.255.255 • POS0/0: J.2.0.245 255.255.255.252 • POS0/1: J.2.182.1 255.255.255.240 • POS0/2: J.2.192.1 255.255.255.240 • POS1/0: J.2.0.14 255.255.255.252 • POS2/0: J.2.0.22 255.255.255.252 • POS4/0: J.2.0.33 255.255.255.252 • GigabitEthernet6/1.330: J.2.11.1 255.255.255.248 • GigabitEthernet6/1.340: J.2.12.1 255.255.255.0

Configuration Files

```
version 12.0
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
!
hostname ISP2BB3
!
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication login NOTACACS enable
aaa accounting exec default start-stop tacacs+
```

```
aaa accounting commands 0 default start-stop tacacs+
aaa accounting commands 15 default start-stop tacacs+
enable password lab
!
clock timezone PDT -8
clock summer-time PDT recurring
!
!
!
ip subnet-zero
ip domain-name isp2.com
ip name-server J.4.7.10
ip multicast-routing distributed
clns routing
!
!
interface Loopback0
 ip address J.2.0.203 255.255.255.255
 no ip directed-broadcast
 ip pim sparse-mode
 ip router isis
 ip mroute-cache distributed
!
interface POS0/0
 description TO ISP3BB7, POS12/0/0
 ip address J.2.0.245 255.255.255.252
 no ip directed-broadcast
 ip pim bsr-border
 ip pim sparse-mode
 ip multicast boundary 1
 ip router isis
 ip mroute-cache distributed
 crc 16
 clock source internal
!
interface POS0/1
ip address J.2.182.1 255.255.255.240
 no ip directed-broadcast
 ip router isis
 no ip mroute-cache
 no keepalive
 crc 16
 clock source internal
!
interface POS0/2
ip address J.2.192.1 255.255.255.240
 no ip directed-broadcast
 ip router isis
 no ip mroute-cache
 no keepalive
 crc 16
 clock source internal
!
interface POS1/0
 description TO ISP2BB1/0, POS 3/0
 ip address J.2.0.14 255.255.255.252
 ip pim sparse-mode
 ip router isis
 ip mroute-cache distributed
 load-interval 30
 crc 32
 clock source internal
!
```

```
!
access-list 1 deny   224.0.1.39
access-list 1 deny   224.0.1.40
access-list 1 deny   239.0.0.0 0.255.255.255
access-list 1 permit any
access-list 124 deny   ip any host 224.0.2.2
access-list 124 deny   ip any host 224.0.1.3
access-list 124 deny   ip any host 224.0.1.24
access-list 124 deny   ip any host 224.0.1.22
access-list 124 deny   ip any host 224.0.1.2
access-list 124 deny   ip any host 224.0.1.35
access-list 124 deny   ip any host 224.0.1.60
access-list 124 deny   ip any host 224.0.1.39
access-list 124 deny   ip any host 224.0.1.40
access-list 124 deny   ip any 239.0.0.0 0.255.255.255
access-list 124 deny   ip 10.0.0.0 0.255.255.255 any
access-list 124 deny   ip 127.0.0.0 0.255.255.255 any
access-list 124 deny   ip 172.16.0.0 0.15.255.255 any
access-list 124 deny   ip 192.168.0.0 0.0.255.255 any
access-list 124 deny   ip any 232.0.0.0 0.255.255.255
access-list 124 permit ip any any
snmp-server engineID local 00000090920000024ADFB800
snmp-server community public RO
snmp-server community STSS RW
snmp-server packetsize 2048
snmp-server contact sysadmin
snmp-server chassis-id ISP1AC1
!
tacacs-server host 223.255.254.254 key cisco12345
tacacs-server key cisco12345
!
alias exec int_desc show int | include Description
alias exec cpu show proc cpu | include CPU
alias exec mem show mem free | include Processor
!
line con 0
 exec-timeout 0 0
 login authentication NOTACACS
 transport input none
line aux 0
 exec-timeout 0 0
line vty 0 4
 exec-timeout 0 0
 password lab
line vty 5 15
!
ntp clock-period 17180286
ntp update-calendar
ntp server 223.255.254.254 version 1
end
```

```
interface POS2/0
 description TO ISP2BB2, POS3/0
 ip address J.2.0.22 255.255.255.252
 ip pim sparse-mode
 ip router isis
 ip mroute-cache distributed
 crc 32
 clock source internal
!
interface POS4/0
 ip address J.2.0.33 255.255.255.252
 ip pim sparse-mode
 ip router isis
 ip mroute-cache distributed
 crc 32
 clock source internal
!
interface GigabitEthernet6/0
 no ip address
 no ip directed-broadcast
 no negotiation auto
!
interface GigabitEthernet6/1.330
 description To Client/Server
 encapsulation dot1Q 330
 ip address J.2.11.1 255.255.255.248
 ip pim sparse-mode
 ip router isis
!
interface GigabitEthernet6/1.340
 description OPEN
 encapsulation dot1Q 340
 ip address J.2.12.1 255.255.255.0
 ip pim sparse-mode
 ip router isis
!
interface GigabitEthernet6/1.350
 encapsulation dot1Q 350
 ip pim sparse-mode
!
router isis
 net 49.0002.0000.0000.0003.00
 is-type level-1
!
router bgp 2
 no synchronization
 redistribute connected
 neighbor ISP2INTERNAL peer-group nlri unicast multicast
 neighbor ISP2INTERNAL remote-as 2
 neighbor ISP2INTERNAL update-source Loopback0
 neighbor ISP2INTERNAL route-map connected-bgp out
 neighbor ISP2ISP3PEER peer-group nlri unicast multicast
 neighbor ISP2ISP3PEER remote-as 3
 neighbor J.2.0.201 peer-group ISP2INTERNAL
 neighbor J.2.0.202 peer-group ISP2INTERNAL
 neighbor J.2.0.204 peer-group ISP2INTERNAL
 neighbor J.2.0.205 peer-group ISP2INTERNAL
 neighbor J.2.0.206 peer-group ISP2INTERNAL
 neighbor J.2.0.207 peer-group ISP2INTERNAL
 neighbor J.2.0.208 peer-group ISP2INTERNAL
 neighbor J.2.0.246 peer-group ISP2ISP3PEER
 no auto-summary
!
no ip classless
```

```
ip http server
ip http authentication local
ip pim rp-address J.2.0.124
ip pim accept-register list no-ssm-range
!
!
ip access-list extended no-ssm-range
 deny   ip any 232.0.0.0 0.255.255.255
 permit ip any any
logging trap emergencies
access-list 1 deny   224.0.1.39
access-list 1 deny   224.0.1.40
access-list 1 deny   239.0.0.0 0.255.255.255
access-list 1 permit any
access-list 10 permit J.2.11.1
access-list 20 permit J.2.11.9
access-list 69 permit J.2.11.0 0.0.0.255
access-list 69 deny   any
access-list 112 deny   ip 223.0.0.0 0.255.255.255 255.255.0.0 0.0.255.255
access-list 112 permit ip any any
access-list 124 deny   ip any 229.0.0.0 0.255.255.255
access-list 124 deny   ip any 239.0.0.0 0.255.255.255
access-list 124 permit ip any any
snmp-server engineID local 000000090200001O1F453CC0
snmp-server community public RO
snmp-server community STSS RW
snmp-server contact sysadmin
snmp-server chassis-id ISP2BB3
route-map connected-bgp permit 10
 match ip address 112
 set ip next-hop J.2.0.203
 set origin igp
!
tacacs-server host 223.255.254.254
tacacs-server key cisco12345
!
!
line con 0
 exec-timeout 0 0
 login authentication NOTACACS
 transport input none
line aux 0
line vty 0 4
 exec-timeout 0 0
 password lab
!
ntp clock-period 17180140
ntp update-calendar
ntp server 223.255.254.254 version 1
end
```

ISP1BB3

Device Characteristics

Table 3 shows the device characteristics for ISP1BB3

Table 3 Hardware and Software Device Characteristics for ISP1BB3

Host name	ISP1BB3
Chassis type	Cisco 7513 router
Physical interfaces	• 4 Ethernet/IEEE 802.3 • 1 Fast Ethernet/IEEE 802.3 • 5 Packet Over SONET (POS)
Hardware components	• Cisco Route/Switch Processor Version 2 (RSP2) (R4700) • 6 Versatile Interface Processor Version 2 (VIP2) controllers (1 Fast Ethernet) (4 Ethernet) (5 POS)
Software loaded	Cisco IOS Release 12.1(5)T
Memory	Cisco RSP2 (R4700) processor: 128 MB
IP addresses	• Loopback0: J.1.0.203 255.255.255.255 • Loopback1: J.1.0.100 255.255.255.255 • Ethernet0/0/2: J.1.6.1 255.255.255.248 • FastEthernet0/1/0: J.1.99.1 255.255.255.248 • POS1/0/0: J.1.0.2 255.255.255.252 • POS1/1/0: J.1.0.14 255.255.255.252 • POS3/0/0: J.1.0.17 255.255.255.252 • POS8/1/0: J.4.0.34 255.255.255.252

Configuration Files

```
!
! Last configuration change at 21:28:37 PDT Wed Dec 20 2000
! NVRAM config last updated at 16:19:09 PDT Thu Dec 7 2000 by Scripts
!
version 12.1
service timestamps debug datetime localtime
service timestamps log datetime localtime
service udp-small-servers
service tcp-small-servers
!
hostname ISP1BB3
!
logging buffered 10000 debugging
logging rate-limit console 10 except errors
no logging console
aaa new-model
aaa group server tacacs+ E2EST
  server 223.255.254.254
!
aaa authentication login default group E2EST enable
aaa authentication login NOTACACS enable
```

```
aaa accounting exec default start-stop group E2EST
aaa accounting commands 0 default start-stop group E2EST
aaa accounting commands 15 default start-stop group E2EST
aaa accounting system default start-stop group E2EST
enable password lab
!
clock timezone PDT -8
clock summer-time PDT recurring
ip subnet-zero
ip cef distributed
ip domain-name isp1.com
ip host tftpserv 223.255.254.254
ip name-server J.4.7.10
!
ip multicast-routing distributed
clns routing
no tag-switching advertise-tags
no tag-switching ip
!
!
interface Loopback0
  ip address J.1.0.203 255.255.255.255
  ip directed-broadcast
  ip router isis
  ip pim sparse-mode
!
interface Loopback1
  ip address J.1.0.100 255.255.255.255
  ip router isis
  ip pim sparse-mode
!
interface Ethernet0/0/2
  description TO ISP1BB3CL1
  ip address J.1.6.1 255.255.255.248
  ip router isis
  ip pim sparse-mode
  ip route-cache distributed
  ip mroute-cache distributed
  ip urd
  load-interval 30
!
interface FastEthernet0/1/0
  description to isp1bb3ce FA1
  ip address J.1.99.1 255.255.255.248
  ip router isis
  ip pim sparse-mode
  ip route-cache distributed
  ip mroute-cache distributed
  no keepalive
  full-duplex
!
interface POS1/0/0
  description TO ISP1BB1, POS 1/2
  ip address J.1.0.2 255.255.255.252
  ip router isis
  ip pim sparse-mode
  ip route-cache distributed
  ip mroute-cache distributed
  clock source internal
!
interface POS1/1/0
  description TO ISP1BB2, POS 2/0
  ip address J.1.0.14 255.255.255.252
  ip router isis
```

```
 ip pim sparse-mode
 ip route-cache distributed
 ip mroute-cache distributed
 clock source internal
!
interface POS3/0/0
 description TO ISP1BB4, POS 2/0/0
 ip address J.1.0.17 255.255.255.252
 ip router isis
 ip pim sparse-mode
 ip route-cache distributed
 ip mroute-cache distributed
 clock source internal
!
interface POS8/1/0
 description TO ISP4BB4, POS 12/0/0
 ip address J.4.0.34 255.255.255.252
 ip router isis
 ip pim bsr-border
 ip pim sparse-mode
 ip multicast boundary 10
 ip route-cache distributed
 ip mroute-cache distributed
 clock source internal
!
router isis
 net 49.0001.0000.0000.0003.00
 is-type level-1
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 redistribute connected
 neighbor ISP1INTERNAL peer-group
 neighbor ISP1INTERNAL remote-as 1
 neighbor ISP1INTERNAL update-source Loopback0
 neighbor ISP1INTERNAL route-map connected-bgp out
 neighbor ISP4ISP1PEER peer-group
 neighbor ISP4ISP1PEER remote-as 4
 neighbor J.1.0.200 peer-group ISP1INTERNAL
 neighbor J.1.0.201 peer-group ISP1INTERNAL
 neighbor J.1.0.202 peer-group ISP1INTERNAL
 neighbor J.1.0.204 peer-group ISP1INTERNAL
 neighbor J.1.0.205 peer-group ISP1INTERNAL
 neighbor J.1.0.208 peer-group ISP1INTERNAL
 neighbor J.1.0.209 peer-group ISP1INTERNAL
 neighbor J.1.0.210 peer-group ISP1INTERNAL
 neighbor J.4.0.33 peer-group ISP4ISP1PEER
 no auto-summary
 !
 address-family ipv4 multicast
 redistribute connected route-map connected-bgp
 neighbor ISP1INTERNAL activate
 neighbor ISP4ISP1PEER activate
 neighbor J.1.0.200 activate
 neighbor J.1.0.201 activate
 neighbor J.1.0.202 activate
 neighbor J.1.0.204 activate
 neighbor J.1.0.205 activate
 neighbor J.1.0.208 activate
 neighbor J.1.0.209 activate
 neighbor J.1.0.210 activate
 neighbor J.4.0.33 activate
 exit-address-family
```

```
!
no ip classless
ip http server
ip pim rp-address J.1.0.100
ip pim accept-register list no-ssm-range
ip msdp peer K.250.1.2 connect-source Loopback0
ip msdp sa-filter in K.250.1.2 list 124
ip msdp sa-filter out K.250.1.2 list 124
ip msdp peer J.4.0.203 connect-source Loopback0 remote-as 4
ip msdp sa-filter in J.4.0.203 list 124
ip msdp sa-filter out J.4.0.203 list 124
ip msdp sa-request J.4.0.203
ip msdp peer J.1.0.204 connect-source Loopback0
ip msdp sa-filter in J.1.0.204 list msdp-nono-list
ip msdp sa-request J.1.0.204
ip msdp cache-sa-state
ip msdp redistribute list msdp-nono-list
ip msdp originator-id Loopback0
!
!
ip access-list extended msdp-nono-list
  deny   ip any 232.0.0.0 0.255.255.255
  permit ip any any
ip access-list extended no-ssm-range
  deny   ip any 232.0.0.0 0.255.255.255
  permit ip any any
logging K.50.0.2
access-list 10 deny   224.0.1.39
access-list 10 deny   224.0.1.40
access-list 10 deny   239.0.0.0 0.255.255.255
access-list 10 permit any
access-list 22 permit 232.0.0.0 0.255.255.255
access-list 22 deny   any
access-list 112 deny   ip 223.0.0.0 0.255.255.255 255.255.0.0 0.0.255.255
access-list 112 permit ip any any
access-list 124 deny   ip any host 224.0.2.2
access-list 124 deny   ip any host 224.0.1.3
access-list 124 deny   ip any host 224.0.1.24
access-list 124 deny   ip any host 224.0.1.22
access-list 124 deny   ip any host 224.0.1.2
access-list 124 deny   ip any host 224.0.1.35
access-list 124 deny   ip any host 224.0.1.60
access-list 124 deny   ip any host 224.0.1.39
access-list 124 deny   ip any host 224.0.1.40
access-list 124 deny   ip any 239.0.0.0 0.255.255.255
access-list 124 deny   ip 10.0.0.0 0.255.255.255 any
access-list 124 deny   ip 127.0.0.0 0.255.255.255 any
access-list 124 deny   ip 172.16.0.0 0.15.255.255 any
access-list 124 deny   ip K.168.0.0 0.0.255.255 any
access-list 124 deny   ip 232.0.0.0 0.255.255.255 any
access-list 124 permit ip any any
route-map connected-bgp permit 10
  match ip address 112
  set origin igp
!
snmp-server engineID local 000000090200001000DDEE000
snmp-server community public RO
snmp-server community STSS RW
snmp-server packetsize 2048
snmp-server contact sysadmin
snmp-server chassis-id ISP1BB3
!
tacacs-server host 223.255.254.254
tacacs-server key cisco12345
```

```
!
line con 0
  exec-timeout 0 0
  login authentication NOTACACS
  length 40
  transport input none
line aux 0
line vty 0 4
  exec-timeout 0 0
  password lab
!
ntp clock-period 17180261
ntp update-calendar
ntp server 223.255.254.254 version 1
end
```

Related Documents

- *Interdomain Multicast Solutions*, Cisco integration solutions document
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/mcst_p1/index.htm
- *Gaining New Efficiencies in Multicast Service Delivery*, Cisco Beyond Basic IP Newsletter V1.36
  http://www.cisco.com/warp/public/779/servpro/promotions/bbip/volume_01_issue36.html
- *Source Specific Multicast with IGMPv3, IGMP v3lite, and URD*, Cisco IOS Release 12.1(5)T feature module
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtssm5t.htm
- *IGMP Version 3*, Cisco IOS Release 12.1(5)T feature module
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtigmpv3.htm
- *Multiprotocol BGP Extensions for IP Multicast*, Cisco IOS Release 12.0(7)T feature module
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/mbgp.htm
- *Changes in MBGP Commands Between 12.0S and 12.0T/12.1*, Cisco Application Note
  http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/mcb12_an.htm
- *Multicast Source Discovery Protocol SA Filter Recommendations*, Cisco Tech Note
  http://www.cisco.com/warp/public/105/49.html
- *IP Multicast Technology Overview*, Cisco white paper
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/mcst_sol/mcst_ovr.htm
- *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.1
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/index.htm
- *Cisco IOS IP and IP Routing Command Reference*, Release 12.1
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_r/index.htm
- Cisco IOS Software IP Multicast Group External Homepage
  ftp://ftpeng.cisco.com/ipmulticast/index.html
- Cisco IOS Software Multicast Services Web Page
  http://www.cisco.com/go/ipmulticast
- RFC 1112, *Host extensions for IP multicasting*
- RFC 2770, *GLOP Addressing in 233/8*